BIG DATA ED INTERNET DELLE COSE: QUALE DESTINO PER LA TUTELA DELLA PRIVACY

CARLOALBERTO GIUSTI

SOMMARIO: 1. Introduzione. - 2. La tutela della privacy nell'era dei "Big Data" e dell'"Internet of things": profili problematici. - 3. Big Data: profili problematici con riferimento alla disciplina del diritto d'autore e dei diritti di proprietà industriale. - 4. Il danno discriminatorio da Big Data. - 5. Conclusioni.

1. Il Parlamento Europeo, in data 14 Aprile 2016, ha approvato definitivamente, dopo un *iter* legislativo durato oltre quattro anni, il c.d. "pacchetto protezione dati", che si compone di un nuovo regolamento concernente la "*tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*", volto a disciplinare i trattamenti di dati personali, sia nel settore privato, sia nel settore pubblico, e destinato ad abrogare la direttiva 95/46/CE. Direttiva che, fino ad oggi, ha costituito il testo di riferimento – a livello europeo – in materia di protezione dei dati personali[1].

Il Regolamento 679/16 è entrato in vigore in data 24 maggio 2016 e diventerà definitivamente applicabile in tutto il territorio UE a partire dal 25 maggio 2018.

La genesi della nuova normativa va ricercata, da una parte, nell'aumento esponenziale delle attività di raccolta e di condivisione dei dati, sia ad opera di soggetti pubblici che privati; nonché, dall'altra, nel repentino sviluppo delle nuove tecnologie che ha facilitato e moltiplicato le occasioni di circolazione delle informazioni relative agli individui, che spesso pubblicano in prima persona, più o meno consapevolmente, i propri dati personali.

Evoluzione che ha dunque reso necessario andare oltre la precedente disciplina: il Regolamento 679/2016 si propone, invero, di assicurare un livello coerente di protezione, di garantire certezza e trasparenza nel trattamento delle informazioni, di offrire diritti azionabili ed obblighi omogenei tra gli Stati, di assicurare un controllo ed una cooperazione efficace tra le Autorità competenti. Finalità che cerca di raggiungere attraverso il rafforzamento dei diritti degli interessati, a fronte di una semplificazione degli adempimenti incombenti sui Titolari del trattamento.

Una delle principali caratteristiche del nuovo regolamento concerne senz'altro il suo ambito di applicazione. Il nuovo regolamento rovescia, invero, il tradizionale principio di stabilimento, sancendo l'applicabilità della disciplina da questo dettata "*indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*" ed individua, quali destinatari delle proprie norme, i titolari e responsabili non stabiliti nell'UE che: (i) trattino dati personali di persone fisiche che si trovano nell'UE quando il trattamento è in relazione a offerte di beni e servizi, indipendentemente dal fatto che sia richiesto o meno un pagamento; o (ii) effettuino attività di

[1] Come noto, in Italia, la disciplina della protezione dei dati personali è dettata dal d.lgs. n. 196 del 30 giugno 2003 ("Codice della privacy"), il cui testo ricalca quello della direttiva n. 95/46/CE (successivamente integrata, per quanto concerne il trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche, dalla direttiva 2002/58/CE).

monitoraggio sul comportamento di persone fisiche che si trovano nell'UE nella misura in cui tale comportamento avvenga nell'UE[2].

Questo il contesto normativo attuale, ci si chiede quale sia effettivamente la tutela prevista a protezione del diritto alla privacy, avuto altresì riguardo alla relazione esistente e sempre più determinate, nella c.d. era digitale, tra il diritto in questione, per l'appunto, ed il mondo degli oggetti di uso quotidiano "intelligenti" (*Internet of Things*, IoT), ovvero il processo di raccolta online delle infinite quantità di dati prodotti a grande velocità da numerosi tipi di fonti, i c.d. "Big Data".

In altre parole, nell'ambito del "subconscio digitale", l'utente – consumatore (ovvero il cittadino in ambito pubblico) potrebbe essere e restare ignaro di quali trattamenti dei suoi dati siano eseguiti da parte di soggetti terzi; non solo: potrebbe ignorare le logiche e i criteri seguiti per quei trattamenti di dati, a mezzo di algoritmi; ed altresì: visto che l'analisi dei *Big Data*, cioè di enormi moli di dati relativi a un singolo *target*, normalmente genera anche dati del tutto nuovi, ulteriori rispetto a quelli già esistenti al momento della raccolta (in quanto frutto di elaborazioni algoritmiche), l'utente potrebbe perfino non sospettare l'esistenza di ulteriori informazioni generate su di sé, magari sensibilissime.

Tali dati possono divenire oltre che una risorsa economica per le aziende anche un'arma contro l'utente stesso (si pensi agli attacchi hacker, ai furti d'identità online, ecc.).

Ebbene, proprio all'interno di tale scenario sta avanzando sempre di più il dibattito sulla tutela della privacy[3]; dibattito molto acceso quando si parla della monetizzazione dei dati e,

---

[2] Quanto agli ulteriori principali tratti modificativi delle disposizioni del regolamento de quo rispetto alla disciplina precedente, è necessario rappresentare che la nuova disciplina ridefinisce le figure di "titolare e responsabile" attribuendo loro obblighi ulteriori rispetto a quanto previsto dalla direttiva 95/46 e dal Codice *Privacy*. La non concretezza e l'inefficienza delle *policies* costituisce per il Titolare fonte di responsabilità (principio di rendicontazione o di "*accountability*", artt. 24 e 32). Con il Nuovo Regolamento il Titolare ha un ruolo più proattivo e obblighi più pregnanti, finalizzati non soltanto al formalistico rispetto delle regole, ma anche all'adozione di tutti gli accorgimenti tecnici e organizzativi necessari a garantire la *compliance* effettiva dei trattamenti sotto il profilo della sicurezza.
Il legislatore europeo dedica altresì una sezione del nuovo regolamento alla "trasparenza" (Sezione 1 del Capo III) e, con riferimento alle modalità di trattamento dei dati, richiede che le informazioni all'interessato:
(i) siano rese con un linguaggio semplice e chiaro, soprattutto nel caso di minori;
(ii) abbiano sempre forma scritta, l'informativa in forma orale essendo ammessa solo quando ciò è richiesto dall'interessato e l'identità di questi possa essere provata con altri mezzi;
(iii) prevedano, *inter alia*, (i) il periodo di conservazione dei dati personali, (ii) il diritto di proporre reclamo ad un'autorità di controllo, (iii) l'intenzione del titolare di trasferire dati personali a un paese terzo.
Parimenti innovativo, è il riconoscimento su base legislativa del diritto all'oblio (art. 17). Fino a oggi questo diritto è stato un prodotto dell'elaborazione giurisprudenziale, dalla quale era definito come il diritto dell'individuo ad essere "dimenticato" dalle banche dati, dai mezzi di informazione, o dai motori di ricerca. In particolare, l'interessato ha diritto di chiedere che siano cancellati e non più sottoposti a trattamento i suoi dati personali
(i) che non siano più necessari per le finalità per le quali sono stati raccolti;
(ii) quando abbia ritirato il consenso o si sia opposto al trattamento o il trattamento dei dati personali non sia altrimenti conforme al Nuovo Regolamento.
La norma *de qua*, menziona tuttavia anche alcuni casi in cui il diritto all'oblio non sussiste; ad esempio, i casi in cui il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione o per l'adempimento di un obbligo legale.

[3] Per un'analisi più approfondita sulla tutela della privacy, si rinvia a S. SICA, V. D'ANTONIO, G.M. RICCIO, *La nuova disciplina europea della privacy*, Cedam, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: dalla direttiva 95/46 al nuovo regolamento europeo*, Giappichelli, 2016; L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016.

soprattutto, quando è la privacy stessa che diviene risorsa economica, ovvero quando sono gli utenti stessi a cederla in cambio di servizi gratuiti.

Oggetto della presente trattazione – dopo una concisa disamina dell'attuale panorama legislativo comunitario – è quello di evidenziare l'impatto che lo sfruttamento dei c.d. Big data ha non solo nell'ambito della tutela della privacy, ma anche in quella della tutela del diritto della proprietà industriale e diritto d'autore.

2. L'espressione "Internet delle cose" (*Internet of Things*, IoT)[4] si riferisce all'estensione di internet al mondo degli oggetti e dei luoghi concreti. La presenza negli oggetti di "sensori connessi alla rete (e agli altri oggetti *smart*) permette un trasferimento di dati supportato dalle caratteristiche principali dell'oggetto. L'oggetto infatti riceve *input* che dall'ambiente esterno comunicano i dati acquisiti ad un *server* il quale, dopo un'elaborazione degli stessi, formula "comandi" da inviare all'oggetto *smart* facendo sì che risponda con degli *output* (volti, per esempio, al perfezionamento del servizio svolto dall'oggetto). Centrale, quindi, appare il ruolo della condivisione dei "dati", il carburante per la produzione successiva di informazioni. I dati singolarmente non risultano particolarmente significativi, ma se analizzati in grandi volumi possono portare alla delineazione di modelli e tendenze, ad esempio comportamentali, che sommandosi ad altre fonti di informazioni producono poi la conoscenza. Nel mondo dell'Internet delle cose i dati aumentano continuamente, innescando una serie di progressi importanti anche da un punto di vista economico. Non a caso, infatti, l'economista Jeremy Rifkin parla ormai da tempo di "terza rivoluzione industriale" riferendosi all'era digitale, un'epoca che porta con sé la presenza sulle piattaforme dell'IoT di dati che incidono significativamente sulla "catena del valore" (*value chain*), in quanto attraverso lo studio delle informazioni presenti si potranno andare a creare applicazioni in grado di aumentare l'efficienza aggregata. Questa condivisione di informazioni, del tutto gratuita, sta sviluppando la cosiddetta *sharing economy*, che potrebbe avere conseguenze inaspettate per la crescita dei Paesi in via di sviluppo, fornendo loro quel "bagaglio di informazioni" finalizzato alla risoluzione di alcuni dei problemi che si trovano ad affrontare"[5].

Se si parla di Internet delle cose, non si può prescindere dal fenomeno dei "*Big data*", in quanto il primo genera i secondi.

I *Big data* sono considerati come i "giacimenti petroliferi del Terzo Millennio"[6] e, nello specifico, definiti dalla Commissione Europea come «*una grande quantità di tipi diversi di dati*

[4] Per un'analisi più approfondita del fenomeno degli IoT, si veda: A. MCEWEN, H. CASSIMALLY, *L'Internet delle cose*, Milano, Apogeo, 2014.

[5] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, in Documenti IAI (Istituto Affari Internazionali), 2016, p. 3, consultabile *on-line*: www.iai.it.

[6] Per la definizione si rinvia a: M.BOGNI, A. DEFANT, *Big Data: diritti IP e problemi della privacy*, in *Il Diritto Industriale*, volume n. 2/2015, p. 117; E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series* n. 6/2017, p. 1, la quale, nel definire i dati come il "nuovo petrolio", *sub* nota 1 riporta integralmente "*L'espressione è riportata in WORLD ECONOMIC FORUM, Personal Data: the emergence of a new asset class, 2011 p. 5 Molteplici sono stati i tentati paragoni volti a definire l'importanza che i dati assumono nella Società dell'Informazione. Qualcuno ne ha paragonato la natura alla seta per la sua capacità di accumularsi come fili nel cyberspazio e di intrecciarsi fino a formare <<un*

prodotti con un'alta velocità da un grande numero di fonti di diverso tipo. La gestione di tali aggregati di dati richiede oggi nuovi strumenti e metodi, come processori potenti, software e algoritmi»[7].

Il valore delle informazioni non è dunque intrinseco, ma dato dalla capacità di organizzarle, analizzarle, misurarle e conseguentemente ricavarne fattori e decisioni. Da ciò deriva che, le attività di analisi dei *Big data* riposano su due piani: *software* e algoritmi per l'analisi, da un lato, e l'insieme dei dati raccolti e aggregati, dall'altro.

Questa la definizione dei *Big data*, ci si chiede come sia possibile proteggerli (anche al fine di incentivarne lo sviluppo), e come proteggere l'utente da essi e dalle loro applicazioni.

Ma vi è di più.

La problematica, in realtà, si fonda su come regolamentare l'informazione nella sua dimensione più pura e nelle sue applicazioni più avanzate, assicurando il giusto equilibrio tra esclusione e accesso[8].

L'informazione rappresenta da sempre una risorsa economica ed essere in grado di analizzare i dati raccolti dagli oggetti *smart* rappresenta una vera e propria sfida da cogliere nell'ambito del settore economico[9].

In termini più pratici, il *data mining* si afferma come uno dei settori più strategici per le aziende che operano nel contesto contemporaneo, le quali possono incrociare dati, avendo l'utente come unità di analisi per scoprire opportunità di investimenti economici enormi[10].

Lo scenario sinora rappresentato solleva diverse problematiche dal punto di vista giuridico[11]: un primo profilo problematico concerne la definizione di "dato" e di "dato

---

arazzo della personalità online dell'utente>> C. MARSDEN, I. BROWN, *"Regulating Code", Boston, 2011. L'OECD ne ha invece sottolineato la natura di infrastruttura per la loro capacità di acquistare valore ogni qual volta riutilizzati e di servire scopi differenti. OECD, Data-driven innovation: Big Data for growth and well-being, Paris, 2015*".

[7] *Towards a thriving data-driven economy* (COM(2014) 442 Final), p. 4.

[8] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, op. cit., p. 2, la quale, sub nota 4 riporta integralmente "*Si veda G. GHIDINI, «Exclusion and Access in Copyright Law: the Unbalanced features of the European Directive of Information Society (INFOSOC)», in Dir. Ind. 2013 p. 6 nota 6, dove, con riferimento al diritto d'autore, accesso e esclusione vengono definiti come "gemelli siamesi" reciprocamente dipendenti*".

[9] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, op. cit., p. 7.

[10] Il concetto di "*Data mining*" è ulteriormente analizzato da Sabrina Palanza, *Internet of things, big data e privacy: la triade del futuro*, op. cit., p. 10, ove l'autrice si sofferma nel dichiarare che "*"Data mining" è il termine con il quale si identificano tutte le tecniche e le metodologie finalizzate all'estrazione di sapere e conoscenza partendo da una vasta mole di dati, e al successivo utilizzo di questo sapere per scopi scientifici, industriali ecc. Oggigiorno, gran parte delle aziende sono impegnate nell'attuazione del data mining, considerandolo un investimento a lungo termine. Ed è proprio l'immensa mole di dati che ormai le aziende si trovano a dover gestire che ha portato allo sviluppo del business analytics. Gli strumenti di quest'ultima metodologia di analisi possono aiutare le aziende ad identificare rapidamente le informazioni importanti (soprattutto per soddisfare l'utente, evitando così di chiedergli dati che poi non sarebbero utilizzati), permettendo così una maggiore trasparenza aziendale e una maggiore condivisione della conoscenza internamente alle aziende stesse*".

[11] Per una disamina sul fenomeno dei c.d. Big Data, si rinvia a ZENO – ZENCOVICH e GIANNONE CODIGLIONE, *Ten legal perspectives on the "Big Data Revolution*", Editoriale Scientifica, 2017. Con riferimento allo scritto in questione, si rinvia altresì a F. DI PORTO (a cura di), *Big data e concorrenza*, *numero speciale di Concorrenza e mercato*, *La rivoluzione Big Data. Un'introduzione*, vol. 23 2016, pp. 5-14. In particolare, l'autrice a p. 13 rappresenta che "*Le "dieci tesi" di Zeno Zencovich e Giannone Codiglione offrono una lettura composita del fenomeno big data da altrettante prospettive giusprivatistiche, includendone una (l'ultima) etica. Accanto agli aspetti proprietari dei big data, ove si richiamano e discutono i tre modelli della proprietà tradizionale, della proprietà intellettuale e del contratto, gli autori sottolineano come la "commodification" dei big data stia sgretolando la nobile tradizione che vede i dati personali appartenenti alla sfera del diritto morale della personalità, non mercificabile, relegandola viepiù ad un mero "wishful thinking". Dalla commerciabilità del sé del "consumatore iper-connesso", gli autori affrontano le questioni poste dalle possibili tipologie contrattuali impiegabili per la trasmissibilità dei dati personali, come di quelli "all'ingrosso". Specie dei primi, si evidenzia come la finzione della "gratuità" di molti servizi online, pagati invece col "prezzo" dei propri dati personali, renderebbe applicabile la disciplina dei contratti del consumatore, con la conseguente nullità di molte delle clausole previste nei terms and conditions delle "app" e dei "social" più diffusi*".

personale". Sono infatti presenti norme che si applicano per i "dati" e norme che si applicano per i "dati personali" e più specificatamente per i "dati sensibili"; altro problema che fa discutere è se rientrino nei "dati" anche i cosiddetti "metadati", ovvero quelle informazioni che associate ad una pagina web, o anche ad una parte di essa, riescono a descriverne il contenuto e il contesto di riferimento[12].

Sulla base delle linee guida Ocse del 1980, rivedute nel 2013[13], sono da definirsi come "dati personali" tutte quelle informazioni relative ad un determinato individuo e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, il suo stato di salute, ecc. A questa definizione, ripresa anche dalla Direttiva 95/46/CE del 1995 (art. 2), segue quella di "dato sensibile" riportata anche dal Codice in materia di protezione dei dati personali italiano (art. 4), ovvero quei dati che possono rivelare l'origine etnica e razziale di una persona, le sue convinzioni religiose, politiche, l'adesione a partiti politici, lo stato di salute e la natura sessuale[14].

Tuttavia, con l'evoluzione tecnologica, altre tipologie di dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche e quelli che consentono la geolocalizzazione, ovvero quei dati che vengono prodotti quotidianamente dagli utenti con l'utilizzo di oggetti *smart*[15].

A tal proposito, il gruppo di esperti Ocse ha suggerito che il termine "dati personali" venga inteso in chiave evolutiva, considerando anche quelle informazioni che, se connesse ad altri dati sull'individuo, possono produrre effetti su di esso, sottolineando l'importanza del modo in cui i dati vengono utilizzati. Questa interpretazione della definizione di "dato personale" è significativa nel momento in cui si parla di "metadati", ovvero quei dati che descrivono in modo strutturato le proprietà dei dati presenti in una pagina web, descrivendone, per esempio, il contenuto e la locazione[16].

Quando si parla di "dati", come ricorda il Garante italiano per la privacy[17], si possono giuridicamente identificare quattro attori principali:

• l'interessato, ovvero la persona fisica cui si riferiscono i dati personali;

• il titolare, ossia la persona fisica, l'azienda, l'ente pubblico ecc. cui spettano le decisioni sugli scopi e sulle modalità del trattamento dei dati, e gli strumenti da utilizzare;

• il responsabile, che può essere una persona fisica, una società, un ente pubblico o un'associazione a cui il titolare affida compiti specifici per il trattamento e controllo dei dati;

• l'incaricato, ovvero colui che per conto del titolare elabora o utilizza, con determinate finalità, i dati, seguendo le direttive del titolare.

---

[12] C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Bologna, Il Mulino, 2015, p. 28.

[13] Garante per la protezione dei dati personali, *Linee guida Privacy Ocse riviste*, 9 settembre 2013, http://www.garanteprivacy.it/garante/doc.jsp?ID=2629667.

[14] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, *op. cit.,* pp. 7-8.

[15] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, *op. cit.,* p. 8.

[16] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, *op. cit.,* p. 8. L'autrice sul punto chiarisce in tal senso: *"Basti pensare ad una libreria digitale contenente diversi dati/oggetti: è proprio grazie ai metadati che è possibile scoprire chi ha creato il dato in analisi, chi lo possiede, quando è stato creato, ecc.".*

[17] Garante per la protezione dei dati personali, *Cosa intendiamo per dati personali?*, http://www.garanteprivacy.it/web/guest/home/diritti/cosa-intendiamo-per-dati-personali.

I problemi principali dovuti alla continua espansione dati prodotta dall'IoT sono due: (i) da un lato quello legato alla protezione dei dati che, se usati abusivamente, possono divenire oltre che una risorsa economica per le aziende anche un'arma contro l'utente stesso; (ii) dall'altro, quello di stabilire e definire con chiarezza i ruoli di coloro che vengono a contatto con i dati stessi[18].

Sotto il profilo della c.d. monetizzazione dei dati, il dibattito è molto acceso, soprattutto quando è la privacy stessa che diviene risorsa economica e quando sono gli utenti stessi a cederla in cambio di servizi gratuiti.

Ad ogni modo, non può non essere rilevato che uno dei cardini su cui non si transige è il c.d. "requisito di avviso e consenso" alla raccolta dei dati, ossia il principio per cui l'utente deve essere avvisato che i suoi dati saranno raccolti. Ciò è ormai previsto dalle norme giuridiche esistenti, ma secondo alcuni giuristi perde di significato nel momento in cui si parla di *big data*. Infatti, per loro natura, questa evoluzione dei dati non è significativa nel momento della raccolta, bensì quando i *big data* vengono analizzati ed archiviati nella loro immensa varietà, velocità e volume[19].

In tale scenario, si propone la questione della configurabilità del dato personale come bene giuridico[20].

A prescindere dal riconoscimento o meno del dato personale alla più ampia categoria di bene giuridico, "non si può certamente negare che la protezione di esso sia da considerarsi come diritto fondamentale, sia alla luce della disciplina Europea che alla luce della nostra carta costituzionale. Poiché non è possibile negare che il dato personale (anche quando inserito all'interno di modalità circolatorie) mantiene un indissolubile legame con il soggetto a cui si riferisce, è necessario che l'assetto normativo si ponga come scopo primario quello di evitare che i diritti della personalità dell'individuo siano colpiti nel loro nucleo fondamentale. Lo scopo deve essere dunque duplice: proteggere la dignità dell'individuo e renderlo partecipe del valore che viene tratto dall'utilizzo dei suoi dati. La tutela del soggetto di diritto nell'ambito dei *Big Data* deve dunque valorizzare il suo rapporto diretto con i dati personali ma deve anche essere tale da assicurargli la possibilità di essere parte stessa del mercato che egli alimenta. Anziché porsi in contrasto, questi due aspetti possono essere ricondotti a un unico principio e cioè la garanzia dell'autonomia dell'individuo rispetto all'utilizzo dei suoi dati personali"[21].

---

[18] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, *op. cit.,* p. 9.

[19] S. PALANZA, *Internet of things, big data e privacy: la triade del futuro*, *op. cit.,* p. 10, la quale sul punto sub nota 24 rinvia a "*Carlo Focarelli, La privacy, cit., p. 70*".

[20] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, op. cit., p. 10, la quale, sub nota 21 riporta integralmente "*Esiste sulla questione un'ampia letteratura che non si limita alla mera contrapposizione tra contrari e favorevoli ma vede declinarsi diverse posizioni e interpretazioni. Si citano qui, tra gli altri, a mero titolo di riferimento* L. MORMILE, "Lo statuto giuridico dei dati personali" in R. PANETTA (a cura di) "Libera circolazione e protezione dei dati personali", 2006, p.531 e ss. A. MANTELERO, "Il costo della privacy tra valore della persona e ragione di impresa", 2007 p.570 ss. In senso più ampio, sull'informazione come bene giuridico: P. PERLINGIERI, «*L'informazione come bene giuridico» in Rass.dir.civ. 1990* e P. CATALA, "Ebauche *d'une teorie jurirdique des productions immatérielles" in "L'appropriation de l'information", 1986*".

[21] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, op. cit., p. 10, la quale sub nota 22 rinvia a O. TENE, J. POLONETSKY, *«Big Data for All: Privacy and Use Control in the Age of Analytics»* in *Northwestern Journal of Technology and Intellectual Property* vol. 11 n. 5, 2013, p. 263, ed anche W. KERBER,

Al fine di garantire che i dati personali non siano soggetti ad accessi o intrusioni anomali, dal punto di vista delle imprese, si contempla il processo che consente di rendere il dato non più identificativo dell'individuo (e, quindi, non più dato personale), tanto da permette ai controllori dei dati di sottrarsi, almeno parzialmente, dagli obblighi scaturenti dalla tutela dei dati personali. Tuttavia, esso non solleva le imprese dei Big Data da ogni onere: è necessario compiere l'accertamento circa la mancata reversibilità di tale processo. Un ulteriore strumento, utilizzabile per proteggere il *data subject* e per attribuirgli dei poteri nell'ambito della gestione dei dati, è la cosiddetta *data portabilità*: *rectius*, attribuendo cioè copia intellegibile dei propri dati raccolti, l'individuo acquista consapevolezza di quanto di proprio è nelle mani del controllore e allo stesso tempo ha facoltà di utilizzarlo come meglio ritiene, esercitando la sua autonomia e partecipando dunque del valore creato dai suoi dati[22].

Affinché ciò si realizzi nell'interesse dell'utente, è necessario aggiungere "un'effettività del principio di trasparenza (la cui importanza è stata, ancora una volta, sottolineata dal nuovo Regolamento UE). Quest'ultimo deve essere visto in senso ampio e, in particolare, in modo tale da investire due differenti profili. Il primo è relativo alla necessità di garantire al soggetto conoscenza su chi sia effettivamente in possesso dei dati personali e sulle modalità con le quali essi sono stati acquisiti, anche e soprattutto quando sono intervenuti scambi con terze parti. Il soggetto dovrebbe (ma ciò non è sempre facile nella pratica) essere in grado di risalire la catena dei passaggi che coinvolgono i suoi dati al fine di poter esercitare i suoi diritti. Dall'altro lato, è necessario che la trasparenza investa anche le modalità con la quale i dati sono trattati e, conseguentemente, gli algoritmi che sottendono l'analisi di essi"[23].

3. Come in precedenza rappresentato, il mondo dei *Big Data* va quindi valutato sulla base dei due piani su cui esso si fonda: gli strumenti di *analytics* e i dati.

Il primo piano è quello relativo alle strutture necessarie per poter efficacemente svolgere le attività di analisi: infrastrutture fisiche e non fisiche tra le quali assumono particolare rilevanza, come detto, i software e gli algoritmi.

A questo punto della trattazione, sarebbe opportuno verificare se e a che livello sia possibile configurare diritti di proprietà intellettuale su questi ultimi elementi, proteggendo il vantaggio competitivo degli operatori e allo stesso tempo stimolando lo sviluppo del settore. Per quanto riguarda i programmi per elaboratori, la protezione principale è assicurata dal diritto d'autore. La tutela di per sé si presenta come particolarmente forte: *erga omnes*, automatica e di lunga durata. Tuttavia, essa non offre una notevole stabilità, richiedendo la sussistenza di un requisito di originalità (inteso in UE come *author's own intellectual creation* e negli US, dopo la

---

"*Digital Markets, Data and Privacy: Competition Law, Consumer Law, and Data Protection* in *Joint discussion Paper Series in Economics*, 14 (2016) p. 10.

[22] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, op. cit., p. 11, la quale sub nota 24 rinvia a O. TENE, J. POLONETSKY, *op. cit.,* p. 263.

[23] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, *op. cit.,* pp. 11-12.

sentenza *Feist*, come *modicum* di creatività) che facilmente può essere negato, ogni qualvolta le istruzioni presenti nel codice siano necessitate dalla funzione[24].

E' necessario anche rappresentare che, "l'applicazione della disciplina brevettuale agli strumenti analitici, pur se riconosciuta, risulterebbe probabilmente inidonea a garantire un effettivo livello di protezione. Il brevetto è, infatti, un diritto di proprietà intellettuale "statico" che, cioè, cristallizza l'invenzione nella sua descrizione. Al contrario, gli strumenti di data analytics, sono tanto più efficaci quanto più in grado di evolversi e di adattarsi nel tempo. La protezione di tali strumenti, tuttavia, può efficacemente basarsi su due tutele diverse: la tutela del segreto industriale e quella contrattuale. Queste ultime hanno entrambe il difetto di essere relative: diritti *in personam* e non *in rem*.

In particolare, moltissimi dubbi possono essere sollevati rispetto all'efficacia del primo metodo. La tutela del *trade secret*, ancorché capace di coprire sia source code che algoritmi, incontra infatti dei limiti: la necessità di provare l'applicazione di misure efficaci per garantire la segretezza (difficile da raggiungere, in un mondo interconnesso e aperto come quelli dei Big Data) e l'impossibilità di proteggersi da atti indipendenti di terzi o da pratiche di *reverse engineering*. In aggiunta, la tutela dei *trade secret* si presenta, più degli altri strumenti di proprietà intellettuale, come fortemente frammentata nei diversi paesi (nonostante la recente direttiva UE che è principalmente volta a garantire l'effettività dei rimedi più che ad armonizzare). In alcuni paesi, il segreto industriale è, infatti, protetto mediante previsioni legislative (in Italia artt. 98 e 99 c.p.i.) mentre in altri (si veda la Germania) esso è ricondotto alla più ampia disciplina dalla concorrenza sleale"[25].

Anche con riferimento ai *dataset* (l'insieme aggregato dei dati sulla base del quale operano le attività di analisi dei *Big Data*), si presenta analoga problematica di protezione della proprietà

---

[24] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, *op. cit.,* p. 3, la quale sub nota 5 riporta integralmente "*Il principio dell'author own intellectual creation è stabilito nelle direttive dell'UE con specifico riferimento a computer programs (dir. 91/250/CE poi modificata da dir. 2009/24/CE) e database (dir.96/9/CE). Tuttavia è bene sottolineare che a seguito della sentenza INFOPAQ (ECJ C-5/08) il criterio deve ritenersi applicabile a tutte le opere di ingegno, in lettura congiunta con la direttiva INFOSOC (dir. 2001/29/CE). Negli USA nella sentenza Feist la Supreme Court ha innalzato il livello di creatività richiesto nella disciplina statunitense superando l'angolosassone approccio dello sweat of the brow (Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991)).*
Tuttavia, si potrebbe ritenere che una forma di protezione potrebbe sorgere in UK, laddove il CDPA sec. 3(1)(a) conserva, nonostante l'intervenuta direttiva a livello europeo, protezione per "a table of compilations other than a database" . Con riferimento a queste ultime, si è sostenuto che la differenza rispetto ai database sia proprio nel livello di originalità richiesto. Le table of compilations conserverebbero, sotto questo punto di vista, la possibilità di applicazione del vecchio approccio cd. sweat of the brow che richiede al fine di stabilimento della tutela la mera presenza skill, labour and judgement (alternativamente). Si veda relativamente alla giurisdizione inglese: T. APLIN, J. DAVID, "Intellectual Property Law: Text, Cases and materials", 2009, Oxford pp. 201 ss.. L'autrice continua sul punto a fornire una disamina del sistema americano, sostenendo, con riferimento alla disciplina brevettuale, che *"A differenza di quanto previsto in Europa, infatti, gli Stati Uniti consentono la protezione dei cosiddetti business method che potrebbero ricomprendere le combinazioni di algoritmi e programmi per elaboratore. Anche in questo senso la strada si presenta in salita. Nel leading case Alice, la Supreme Court ha stabilito che le condizioni che consentono la brevettabilità di tali oggetti sono due: l'invenzione non deve essere solo un'idea astratta e qualora sia tale deve mostrare un passo inventivo ulteriore che applichi tale idea6. La case law statunitense ci mostra che è sempre più difficile la soddisfazione di tali requisiti. In particolare, nella sentenza Content Extractio, la Federal Circuit, applicando il test di Alice e dichiarando l'invalidità del brevetto in questione a causa del suo oggetto astratto, così si esprime: «The concept of data collection, recognition, and storage is undisputedly well-known. Indeed, humans have always performed these functions».*

[25] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, *op. cit.,* p. 4.

intellettuale. Tali dati, infatti, potrebbero essere categorizzati come *database* e quindi soggetti, nell'Unione Europea, al doppio livello di protezione del diritto d'autore e del diritto *sui generis*.

Ebbene, quanto al primo, è ardua la possibilità di configurare la presenza di un livello di originalità tale da poter attrarre la protezione del copyright. Anche in questo caso, il diritto d'autore assicurerebbe protezione dalla sola copia esatta del database (o di parte di esso) come tale. Più appropriato sembra invece il diritto sui generis, sia nella sua costruzione sia nella sua portata. Esso, infatti, sorge a seguito di un sostanziale investimento nell'ottenimento, verificazione e presentazione dei contenuti e permette di proteggere il database dall'estrazione dalla riutilizzazione dei dati[26].

Questa l'analisi dell'istituto che precede, ci si chiede se l'art. 2, comma 9, della Legge sul diritto d'autore (L. 22 aprile 1941, n. 633), che elenca tra le opere dell'ingegno oggetto della protezione di diritto d'autore (e non quindi di un diritto connesso, come invece il diritto sui generis di cui all'art. 102 bis) "le banche dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore", possa attagliarsi alle raccolte di *Big Data*[27].

La risposta non può che essere negativa, dal momento che in tali raccolte il materiale non è "scelto o disposto" dall'autore, ma ricevuto passivamente ed analizzato con l'impegno di programmi per elaboratore, anche se si potrebbe cercare di sostenere che la disposizione dei dati effettuata dal programma debba essere considerata una "creazione intellettuale", legata alla capacità del software di catalogare e correlare i dati in modo originale rispetto alla classificazione che verrebbe ordinariamente operata. Tuttavia, questa lettura non sembra coerente con la *ratio* della norma, che con il requisito della creatività si riferisce al fatto che l'opera costituisca una costruzione ed organizzazione espressiva che rispecchia la personalità dell'autore[28].

Ciò posto, le raccolte di *Big Data* sembrerebbero rientrare nella previsione di cui all'art. 102 bis della Legge sul diritto d'autore, avente ad oggetto le c.d. banche di dati non creative.

Tale disposizione riserva al "costitutore" della banca di dati, da intendersi come "chi effettua investimenti rilevanti per la costituzione di una banca di dati o per la sua verifica o la sua presentazione, impegnando, a tal fine, mezzi finanziari, tempo o lavoro", il diritto di "vietare le operazioni di estrazione ovvero reimpiego della totalità o di una parte sostanziale della stessa". Il diritto *sui generis* viene inquadrato nella categoria dei diritti connessi, categoria residuale nell'ambito del sistema della tutela del diritto d'autore, con contenuto del tutto eterogeneo[29].

La fattispecie costitutiva del diritto *sui generis* si rinviene in presenza di una raccolta di dati "in un momento di un certo rilievo (che tuttavia non è possibile fissare astrattamente), tale

[26] Elisabetta Nunziante, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, *op. cit.,* p. 5.
[27] M. BOGNI e A. DEFANT, *Big Data: diritti IP e problemi della privacy, op. cit.,* p. 119.
[28] M. BOGNI e A. DEFANT, *Big Data: diritti IP e problemi della privacy, op. cit.,* p. 119.
[29] M. BOGNI e A. DEFANT, *Big Data: diritti IP e problemi della privacy, op. cit.,* p. 119.

che il fatto stesso della loro unione soddisfi un bisogno informativo socialmente apprezzabile"[30].

Ebbene, alla luce di tali dati normativi, "le informazioni concernenti l'attività svolta da un utente ad esempio navigando su un sito di e-commerce o su un motore di ricerca rientrano nel complesso di una banca di dati; ed il costitutore di essa (e quindi il gestore del sito o del motore di ricerca stessi) potrà opporsi all'estrazione ed al reimpiego delle stesse ove ciò avvenga nell'ambito di un prelievo che non riguardi solo informazioni singole, ma l'intera banca di dati ovvero una parte sostanziale di essa, e non appena la stessa informazione sarà stata appresa dal sistema e "ordinata in uno o più indici o … accompagnata da codici che ne consentano la catalogazione e il reperimento secondo un criterio prestabilito""[31].

Quella di cui all'art. 102 bis della Legge sul diritto d'autore non è l'unica forma di tutela invocabile per le raccolte di *Big Data*, specie con riferimento alle informazioni aventi ad oggetto le attività svolte dai singoli soggetti sulla rete o comunque informazioni raccolte con strumenti informatici. Invero, possono essere presi in considerazione, anzitutto, le disposizioni di cui agli artt. 98 e 99 c.p.i. che disciplinano il diritto di proprietà industriale sulle informazioni riservate[32].

Quanto ai requisiti di tutela, l'art. 98 c.p.i. prevede che dette informazioni debbano essere:

(i) segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;

(ii) abbiano valore economico in quanto segrete;

(iii) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete.

4. Come abbiamo avuto modo di rappresentare, è possibile che gli strumenti analitici dei *Big Data* (ed in particolare gli strumenti predittivi) si pongano come lesivi della dignità dell'individuo. Attraverso la categorizzazione degli individui all'interno di parametri precostituiti si rischia, infatti, di porre in essere pratiche discriminatorie. Il pericolo è evidente in presenza di dati sensibili ma, a causa del potenziale dell'aggregato, riguarda anche altre tipologie di dati personali. Si pensi, ad esempio, a come tali pratiche possano porsi come lesive dell'individuo nel contesto del lavoro subordinato, quando, mettendo in rapporto poche caratteristiche di un lavoratore e paragonandole ad un pattern, possono essere tratte conclusioni relativamente alla sua condotta sulla base di elementi puramente probabilistici. Ancora, si veda il rischio di colpire

[30] M. BOGNI e A. DEFANT, *Big Data: diritti IP e problemi della privacy, op. cit.,* p. 119, i quali sub nota 2 rinviano a G. Guglielmetti, *La tutela delle banche dati con diritto sui generis nella Direttiva 96/9/CE*, in *Contr. e impr. Europa*, 1997, 181.

[31] M. BOGNI e A. DEFANT, *Big Data: diritti IP e problemi della privacy, op. cit.,* p. 120, i quali sub nota 3 rinviano a G. Guglielmetti, *La tutela delle banche dati con diritto sui generis nella Direttiva 96/9/CE*, op. cit., p. 180.

[32] M. BOGNI e A. DEFANT, *Big Data: diritti IP e problemi della privacy, op. cit.,* pp. 122-123.

la persona nella sua dimensione di consumatore ponendo in essere politiche di discriminazione dei prezzi sulla base delle enormi quantità di dati raccolti[33].

E' evidente che il fiorire di business legati ai *Big Data* si ponga in primo luogo come una minaccia per la protezione dei dati personali e dei principi che si pongono alla base di essa.

I Big Data si inquadrano, infatti, all'interno di un contesto sociale e economico nel quale il meccanismo informazione/consenso mostra sempre più la sua fragilità.

A fronte di forte asimmetrie informative, di una scarsa consapevolezza e dell'urgenza di accedere ai servizi, l'interessato fornisce un consenso la cui natura libera e informata è sempre più questionabile. Dall'altro lato, le stesse imprese, diffidenti della giustificazione del trattamento basato sul consenso, inquadrano sempre più le loro attività in altre condizioni legittimanti[34].

L'arsenale rimediale contemplato nel Regolamento UE 2016/679 in caso di danno discriminatorio può sintetizzarsi nei rimedi esperibili nei confronti: (i) dell'autorità di controllo (artt. 77 – 78); (ii) del titolare del trattamento o del responsabile del trattamento.

In particolare, l'art. *77,* rubricato 'Diritto di proporre reclamo all'autorità di controllo" recita **"***1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione. 2.L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78";* mentre l'art. 78, rubricato 'Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo" dispone che **"**1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda. 2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77. 3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita. 4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

Invece, con riferimento al rimedi contemplati nei confronti del titolare del trattamento o del responsabile del trattamento, l' art. 79 contempla che **"***1. Fatto salvo ogni altro ricorso*

---

[33] Elisabetta Nunziante, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, *op. cit.,* p. 7.

[34] Elisabetta Nunziante, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, *op. cit.,* p. 8, la quale sub nota 8 riporta integralmente che *"Ci si riferisce qui in particolare alle condizioni previste dall'art. 6 co. 1 lett. b) e f) del nuovo Regolamento (Reg. EU 2016/679) e cioè il trattamento necessario per l'esecuzione di un contratto ovvero di misure precontrattuali e il trattamento giustificato da legittimi interessi (in particolare, quest'ultima disposizione si pone come sufficientemente vaga da poter dar luogo ad abusi oltre ad essere contestata per la scelta di porre sullo stesso piano di valutazione interessi e diritti)".*

amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento. 2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri".

Stante il tenore letterale delle suddette previsioni normative, sembrerebbe che il danno discriminatorio da *Big Data* costituisca una preoccupazione prevalente nel Regolamento UE 2016/679.

Tuttavia il sistema di tutele disposto dal legislatore europeo mostrerebbe una rilevante lacuna, laddove contempla il danno discriminatorio esclusivamente con riferimento ai profili di illiceità del trattamento.

In altri termini, se non fosse un trattamento dei dati quello operato dall'algoritmo *Big Data,* ma l'algoritmo de quo venisse utilizzato per fini commerciali da parte di professionisti che si rivolgono a consumatori, *quid iuris*?

Ebbene, trattandosi non solo di potenziale travolgimento della legittimità del trattamento di dati personali in sé, ma anche di impatto sulla opponibilità giuridica "non-privacy" della determinazione commerciale, si potrebbe ipotizzare che la pratica de qua possa rilevare non solo per il Garante Privacy, ma altresì per l'Autorità Garante della Concorrenza e del Mercato.

Invero, il silenzio impercettibile di certe pratiche di analisi di dati, specialmente in ambiente digitale potrebbe infatti consentire al professionista di operare indebiti condizionamenti della scelta (che dovrebbe essere libera e consapevole) del consumatore, verificandosi così una delle pratiche commerciali aggressive di cui all'articolo 25 del Codice del Consumo. Bisognerebbe certamente interrogarsi sull'effettivo grado di "condizionamento" reso possibile sulla base di analisi e profilazioni automatizzate.

In caso di elaborazioni dei dati dei consumatori che portassero a discriminare ingiustificatamente – e soprattutto in modo non trasparente agli occhi del singolo consumatore – l'offerta commerciale a ciascuno di essi riservata, si potrebbe perfino ipotizzare il ricorrere della pratica commerciale scorretta e della ingannevolezza delle comunicazioni.

In presenza di discriminazione commerciale ingiustificata, basata sull'analisi algoritmica automatizzata di Big Data, al di là del Codice del Consumo, ci soccorrerebbe, tra l'altro, l'articolo 14 del Codice Privacy che prevede come l'interessato a cui si riferiscono i dati possa opporsi ad ogni tipo di determinazione (tale potrebbe ben essere un'offerta o un contratto tra professionista e consumatore) fondata unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato "*salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato*" o sulla base di adeguate garanzie individuate dal Garante Privacy.

5. Lo sfruttamento dei *Big Data* costituisce indubbiamente una "rivoluzione" che sta trasformando il nostro modo di vivere, ma che tuttavia minaccia la nostra libertà.

Questo il contesto generale del fenomeno *de quo*, non si può però prescindere dalle effettive problematiche connesse alla tutela della privacy.

Così come non possono sottacersi le manchevolezze della legislazione anti-discriminatoria, fondata su un sistema di accertamento che non sempre assicura un'adeguata protezione alle vittime delle discriminazioni, ostacolandone talvolta *ab origine* l'accesso alla tutela in sede giurisdizionale. Basti pensare, invero, che trascinare un'azienda in tribunale per il risarcimento del danno discriminatorio da *Big Data* significa disporre di risorse economiche di cui spesso il singolo non dispone.

Ma il deludente e scarso sviluppo del contenzioso giudiziale non è solo imputato alla debolezza "economica" dell'iniziativa individuale; non deve infatti essere tralasciata la difficoltà di assolvere l'onere della prova e quello preliminare di allegazione.

Di conseguenza nei fatti l'utente discriminato decide suo malgrado di patire la discriminazione piuttosto che affrontare una guerra giudiziaria che non può permettersi.

Ebbene, nell'ambito della c.d. era digitale – dove praticamente all'utente tutto è concesso, cliccando un semplice tasto – il *deficit* connesso alla tutela delle vittime da danno discriminatorio da *Big Data* non può che costituire un serio ed insostenibile limite.

Lo scenario sinora prospettato si riflette in modo inequivocabile nelle dichiarazioni rese dal Presidente dell'Autorità Garante per la protezione dei dati personali Antonello Soro, secondo il quale "I cambiamenti imposti dall'innovazione tecnologica hanno generato un livello senza precedenti di raccolta e di elaborazione di dati, destinato a subire un'ulteriore espansione con le nuove applicazioni dell'Internet delle cose, della robotica, della realtà aumentata. Dalle parole e dai numeri ai giochi, ai media, alle funzioni complesse dei sistemi industriali, all'ambiente, ai trasporti: tutto quello che riguarda la nostra esistenza ha subito una trasformazione digitale. Ora stiamo varcando una nuova frontiera, stiamo entrando nell'era dei sistemi cognitivi. Una nuova categoria di tecnologie, che utilizza l'elaborazione del linguaggio naturale e dell'apprendimento automatico, è in grado di amplificare e accelerare il processo di trasformazione digitale, per consentire alle persone e alle macchine di interagire in modo più naturale, estendendo e potenziando le competenze e le capacità cognitive. Lo sviluppo delle tecnologie rappresenta il presupposto essenziale perché le imprese possano competere nella dimensione globale dei mercati e perché possano migliorare le condizioni di vita delle persone in ogni angolo del pianeta. Ma i progressi incessanti di questi cambiamenti mettono in discussione molti paradigmi consolidati del diritto e molte consuetudini della politica. E sollevano interrogativi ineludibili. Avvertiamo che lo sviluppo di una florida economia fondata sui dati, che sfrutta le funzionalità tecnologiche per la loro raccolta continua e massiva, la trasmissione istantanea ed il riutilizzo, ci espone a nuovi rischi. E, poiché i dati rappresentano la proiezione digitale delle nostre persone, aumenta in modo esponenziale anche la nostra

vulnerabilità. La libertà di ciascuno è insidiata da forme sottili e pervasive di controllo, che noi stessi, più o meno consapevolmente, alimentiamo per l'incontenibile desiderio di continua connessione e condivisione. Da un lato le imprese tecnologiche hanno dilatato la raccolta e la disponibilità dei nostri dati, dall'altro le esigenze di sicurezza, di fronte alla minaccia criminale e terroristica, hanno spinto progressivamente i governi ad estendere il controllo delle attività svolte in rete per finalità investigative in modo sempre più massivo. Il combinarsi di questi processi ha prodotto una straordinaria intrusione nella vita di tutti, una vera e propria sorveglianza, con effetti importanti sui comportamenti individuali e collettivi, sugli stessi caratteri delle nostre democrazie. Penso che la protezione dei dati debba assumere un ruolo di primo piano per presidiare la dimensione digitale: quella in cui sempre più si dispiega la nostra esistenza e nella quale ora si svolgono anche le relazioni ostili tra gli stati e dentro gli stati. La nuova economia, fatta di tecnologia sempre più interconnessa, favorita dall'espansione dell'Internet in mobilità, alimentata dalla presenza capillare di sensori intelligenti, si caratterizza per i grandi volumi di dati, l'infinita eterogeneità delle fonti da cui provengono e la velocità dei sistemi che li analizzano. Ma governare questi processi non è certamente un compito semplice. La capacità di estrarre dai dati informazioni che abbiano un significato e siano funzionali, richiede infatti lo sviluppo di sofisticate tecnologie e di competenze interdisciplinari che operino a stretto contatto. In questo quadro i progressi nella potenza di calcolo svolgono un ruolo centrale per l'analisi dei Big Data e per l'acquisizione della conoscenza. E in un futuro non troppo lontano l'intelligenza artificiale, grazie ad algoritmi capaci di apprendere e migliorare autonomamente le proprie abilità, offrirà soluzioni efficaci per soddisfare le più disparate esigenze. E arriverà ad occuparsi di problemi che oggi possono sembrare ostacoli insormontabili, a beneficio della collettività (…)"[35].

[35] Si rinvia sul punto all'intervento del Presidente dell'Autorità Garante per la protezione dei dati personali, Antonello Soro, in occasione del Convegno organizzato in occasione della Giornata Europea della protezione dei dati personali – tenutosi in data 30 gennaio 2017 *"BIG DATA E PRIVACY. LA NUOVA GEOGRAFIA DEI POTERI"*, la cui relazione è disponibile sul sito del Garante per la protezione dei dati personali: www.garanteprivacy.it.